

# The Algorithmic Foundations of Data Privacy

Instructor: Aaron Roth

# Administrivia

<http://www.cis.upenn.edu/~aaroht/courses/privacyF11.html>

- Time: Tuesday/Thursday 1:30-3:00
- Room: Here (Towne 315)
- Format:
  - Lectures
  - Student Presentations of Projects
- Evaluation:
  - Class project (60%)
  - Participation (40%)
    - Including blog posts!  
<http://privacyfoundations.wordpress.com/>

# Administrivia

<http://www.cis.upenn.edu/~aaroht/courses/privacyF11.html>

- Project: Semester long study of a topic in privacy
  - Topic suggestions up soon on the website
    - Feel free to pick your own!
  - Can be pure theory, implementation, or somewhere in between
    - Literature review
    - Some component of original research
  - Graded components:
    - Proposal, mid project report, final report and presentation.

# Course Overview

- How can we perform private data analysis?
  - How do we mathematically define “Privacy”?
- How does “privacy” degrade when multiple analyses are performed?
- What are the theoretical limits of how much information we can release about a dataset while preserving “privacy”?

# Course Overview

- How can we design efficient algorithms that make use of data privately?
- How should economic agents reason about their privacy?
  - How should we design auctions and other mechanisms for privacy-aware consumers?

# Today

- Some motivation
- The definition of differential privacy
- An overview of topics we will cover
- If there is time: A lower bound.

# Warning

- Powerpoint: I will probably go too fast
- Stop me! Ask questions!
  - Other people probably have the same question.
  - I will be suspicious if you don't...
  - Remember participation is 40% of your grade!

# A Dilemma





# Modern Algorithm Design

- Computation is not the only constraint
- Dealing with large datasets
  - Data *belongs* to other people
  - Must protect their privacy
  - Must convince them to report it truthfully

# Modern Algorithm Design

- Use search logs to recommend query completions




why is



























[Advanced Search](#)  
[Language Tools](#)

why is **the sky blue**  
why is **my poop green**  
why is **it called black friday**  
why is **everyone posting colors on facebook**  
why is **a raven like a writing desk**  
why is **yawning contagious**  
why is **haiti so poor**  
why is **the world going to end in 2012**  
why is **my computer so slow**  
why is **lil wayne going to jail**

# Modern Algorithm Design

- Find closely connected components in a social network

 **Suggestions**  
Add people you know as friends and become a fan of public profiles you like.

 <b>Joe Locaccino</b> Add as friend	×	 <b>Marie F.</b> Add as friend	×	 <b>Severin Hacker</b> Add as friend	×
 <b>Gregory Sorkin</b> Add as friend	×	 <b>Jim McCann</b> Add as friend	×	 <b>Jonathan Derryberry</b> Add as friend	×
 <b>Andreas Krause</b> Add as friend	×	 <b>Kevin Bierhoff</b> Add as friend	×	 <b>Danny Sleator</b> Add as friend	×
 <b>Ajit Singh</b> Add as friend	×	 <b>Alan Michael Frieze</b> Add as friend	×	 <b>Polo Chau</b> Add as friend	×
 <b>Swapnil Patil</b> Add as friend	×	 <b>Michael Verde</b> Add as friend	×	 <b>Frank Pfenning</b> Add as friend	×
 <b>Johannes Schmieder</b> Add as friend	×	 <b>Benoit Hudson</b> Add as friend	×	 <b>Stephen Magill</b> Add as friend	×
 <b>Nikhil Bansal</b> Add as friend	×	 <b>Dan Licata</b> Add as friend	×	 <b>Colin McMillen</b> Add as friend	×
 <b>Reza Zadeh (Reza Bosagh Zadeh)</b> Add as friend	×	 <b>David Brumley</b> Add as friend	×	 <b>Liz Crawford</b> Add as friend	×
 <b>Himanshu Jain</b> Add as friend	×	 <b>Rob Reeder</b> Add as friend	×		

# Modern Algorithm Design

- Decide which ads to show based on user data and other users previous searches.

The image shows a screenshot of a Google search results page. At the top, the Google logo is on the left, and navigation links for 'Web', 'Images', 'Video', 'News', 'Maps', 'Desktop', and 'more »' are on the right. A search bar contains the text 'FOCS 07' and a 'Search' button. To the right of the search bar are links for 'Advanced Search' and 'Preferences'. Below the search bar, a blue bar indicates 'Web' and 'Results 1 - 10 of about 136,000 for FOCS 07. (0.09 seconds)'. The first search result is titled 'Computational Complexity: FOCS Day 1 and Business Meeting - 2:39pm' and includes a snippet about the event in Providence, RI. Below the snippet are links for 'weblog.fortnow.com/2006/10/focs-day-1-and-business-meeting.html - 34k -', 'Cached', 'Similar pages', and 'Note this'. The second search result is titled 'Computational Complexity: STOC and FOCS' and includes a snippet about the call for papers. Below the snippet are links for 'weblog.fortnow.com/2007/02/stoc-and-focs.html - 28k -', 'Cached', 'Similar pages', 'Note this', and '[ More results from weblog.fortnow.com ]'. On the right side of the page, there is a 'Sponsored Links' section. The first sponsored link is '2007 Fox' with the text 'Make Volkswagen Shopping Easier Compare Your Favorites Side By Side' and the URL 'www.AutoTrader.com'. The second sponsored link is 'Pittsburgh Soda' with the text 'Find soda here! We offer local search in your city' and the URL 'Pittsburgh.Local.com Pittsburgh, PA'. This second sponsored link is enclosed in a blue rounded rectangle.

Google™ [Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [Desktop](#) [more »](#)

[Advanced Search](#)  
[Preferences](#)

**Web** Results 1 - 10 of about 136,000 for FOCS 07. (0.09 seconds)

Computational Complexity: FOCS Day 1 and Business Meeting - 2:39pm  
FOCS 07 will be in Providence, RI. Program chair is Alistair Sinclair. Location is the new Renaissance Hotel, currently under construction. ...  
[weblog.fortnow.com/2006/10/focs-day-1-and-business-meeting.html](http://weblog.fortnow.com/2006/10/focs-day-1-and-business-meeting.html) - 34k -  
[Cached](#) - [Similar pages](#) - [Note this](#)

Computational Complexity: STOC and FOCS  
And in that great circle of theory life, the FOCS '07 Call for Papers is out. Submission deadline is April 20 and FOCS will be held October 21-23 in ...  
[weblog.fortnow.com/2007/02/stoc-and-focs.html](http://weblog.fortnow.com/2007/02/stoc-and-focs.html) - 28k -  
[Cached](#) - [Similar pages](#) - [Note this](#)  
[\[ More results from weblog.fortnow.com \]](#)

Sponsored Links

2007 Fox  
Make Volkswagen Shopping Easier  
Compare Your Favorites Side By Side  
[www.AutoTrader.com](http://www.AutoTrader.com)

Pittsburgh Soda  
Find soda here!  
We offer local search in your city  
[Pittsburgh.Local.com](http://Pittsburgh.Local.com)  
Pittsburgh, PA

# What is Privacy?



# What Isn't Privacy?

- Privacy isn't restricting questions to large populations.
  - “What is the average salary of Penn faculty?”
  - “What is the average salary of Penn faculty not named Aaron Roth?”

# What Isn't Privacy?

- Privacy isn't restricting to “ordinary” facts.
  - Statistics on Alice's bread buying habits: For 20 years she regularly buys bread, and then stops.
    - Type 2 diabetes?

# What Isn't Privacy?

- Privacy isn't "Anonymization"
  - Anonymization is hard.
    - Problem: Auxiliary Information and Linkage Attacks!
    - Case Study: NetFlix Prize Dataset
      - Linked with IMDB database to re-identify users [Narayanan, Shmatikov]
      - 2<sup>nd</sup> Netflix prize cancelled
    - Can't know what the adversary knows, or might know in the *future*.



# What Isn't Privacy?

- Privacy isn't "Anonymization"
  - Anonymization isn't enough
    - Collection of medical records from a specific urgent care center and date might correspond to only a small collection of medical conditions.
    - Knowledge (from a neighbor?) that Alice went to that urgent care center doesn't identify her record, but implies she has one of a small number of conditions.

# What is Privacy?

- Freedom from harm.

Privacy Definition, Attempt 1:

*An analysis of a dataset  $D$  is private if the data analyst knows no more about Alice after the analysis than he knew about Alice before the analysis.*

# What is Privacy

- Problem: Impossible to achieve with auxiliary information.
  - Suppose an insurance company knows that Alice is a smoker.
  - An analysis that reveals that smoking and lung cancer are correlated might cause them to raise her rates!
- Was her privacy violated?
  - This is a problem *even if Alice was not in the database!*
  - This is exactly the sort of information we want to be able to learn...

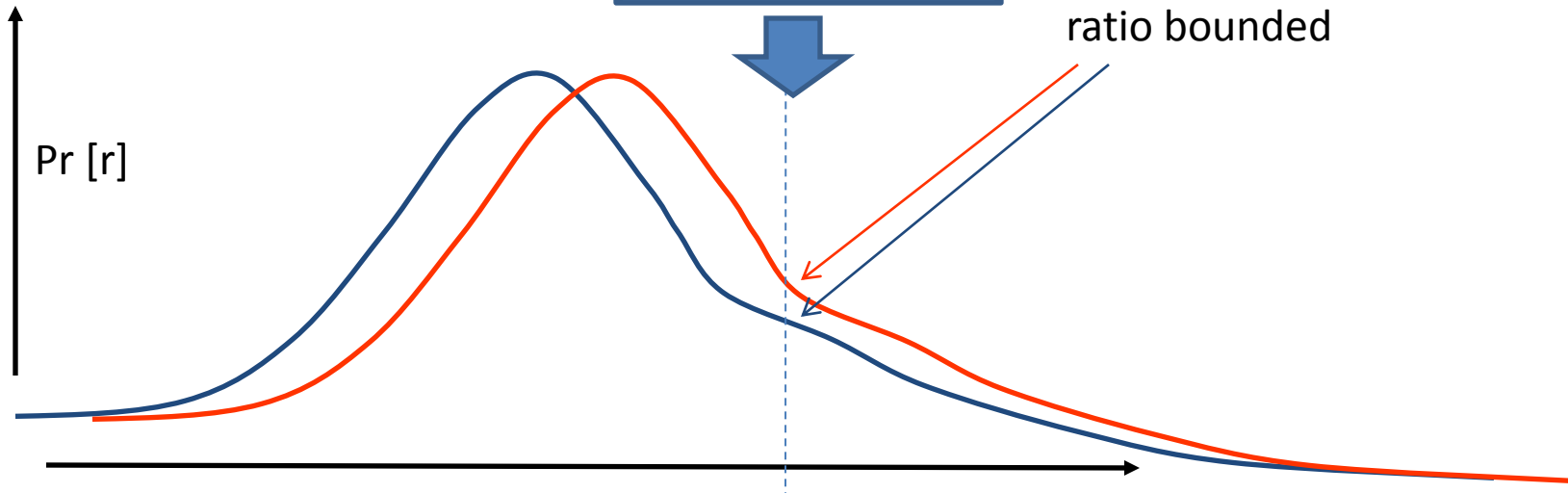
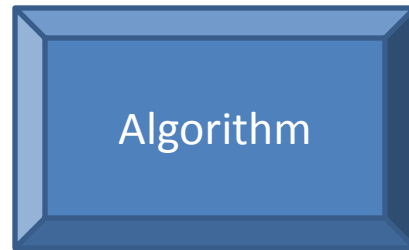
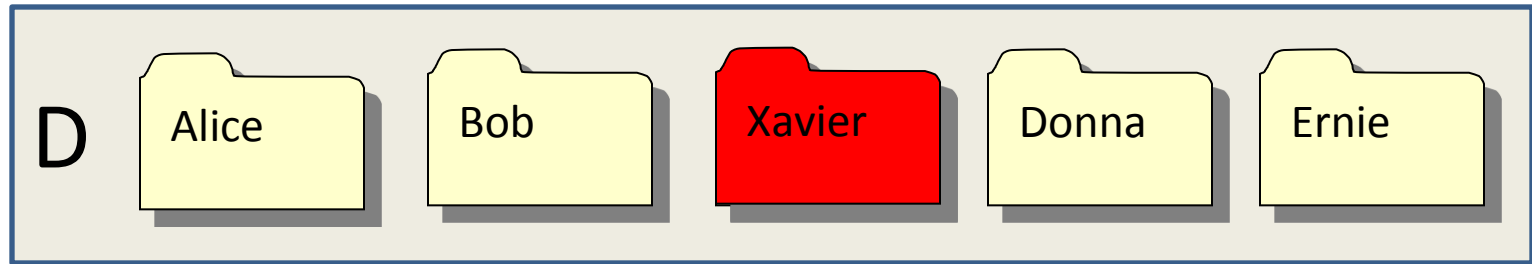
# What is Privacy?

Privacy Definition, Attempt 2:

*An analysis of a dataset  $D$  is private if the data analyst knows **almost** no more about Alice after the analysis than he **would have known had he conducted the same analysis on an identical database with Alice's data removed.***

# Differential Privacy

[Dwork-McSherry-Nissim-Smith 06]



# Differential Privacy

$X$ : The data *universe*.

$D \subset X$ : The dataset (one element per person)

Definition: Two datasets  $D, D' \subset X$  are *neighbors* if they differ in the data of a single individual. i.e.  $|D \Delta D'| \leq 1$ .

# Differential Privacy

$X$ : The data *universe*.

$D \subset X$ : The dataset (one element per person)

Definition: A mechanism  $M: 2^X \rightarrow R$  is  $(\epsilon, \delta)$ -differentially private if for all pairs of neighboring databases  $D, D' \subset X$ , and for all events  $S \subseteq R$ :

$$\Pr[M(D) \in S] \leq e^\epsilon \Pr[M(D') \in S] + \delta$$

$(1 + \epsilon)$

Definition: A mechanism  $M: 2^X \rightarrow R$  is  $(\epsilon, \delta)$ -differentially private if for all pairs of neighboring databases  $D, D' \subset X$ , and for all events  $S \subseteq R$ :

$$\Pr[M(D) \in S] \leq e^\epsilon \Pr[M(D') \in S] + \delta$$

- Think of  $\delta$  as exponentially small (or even 0)
- Think of  $\epsilon$  as a small constant.
  - If  $M: 2^X \rightarrow R$  is  $(\epsilon, 0)$ -DP, and  $|D \Delta D'| = k$ , then:  
$$\Pr[M(D) \in S] \leq e^{\epsilon k} \Pr[M(D') \in S]$$
    - So nothing useful is possible for  $\epsilon = o(\frac{1}{n})$



# Why is Differential Privacy “Privacy”?

- It should guarantee “freedom from harm”
- A useful fact – resilience to post-processing:
  - For any  $f: R \rightarrow R'$ , and any  $(\epsilon, \delta)$ -differentially private  $M: 2^X \rightarrow R$ ,  $f \circ M: 2^X \rightarrow R'$  is also  $(\epsilon, \delta)$ -differentially private.
- What if  $f$  maps mechanism output to events you care about?
  - Differential privacy: “Except for rare events that occur with probability  $\leq \delta$ , your future utility will decrease by at most a  $(1 - \epsilon)$  factor by participating in the database.”

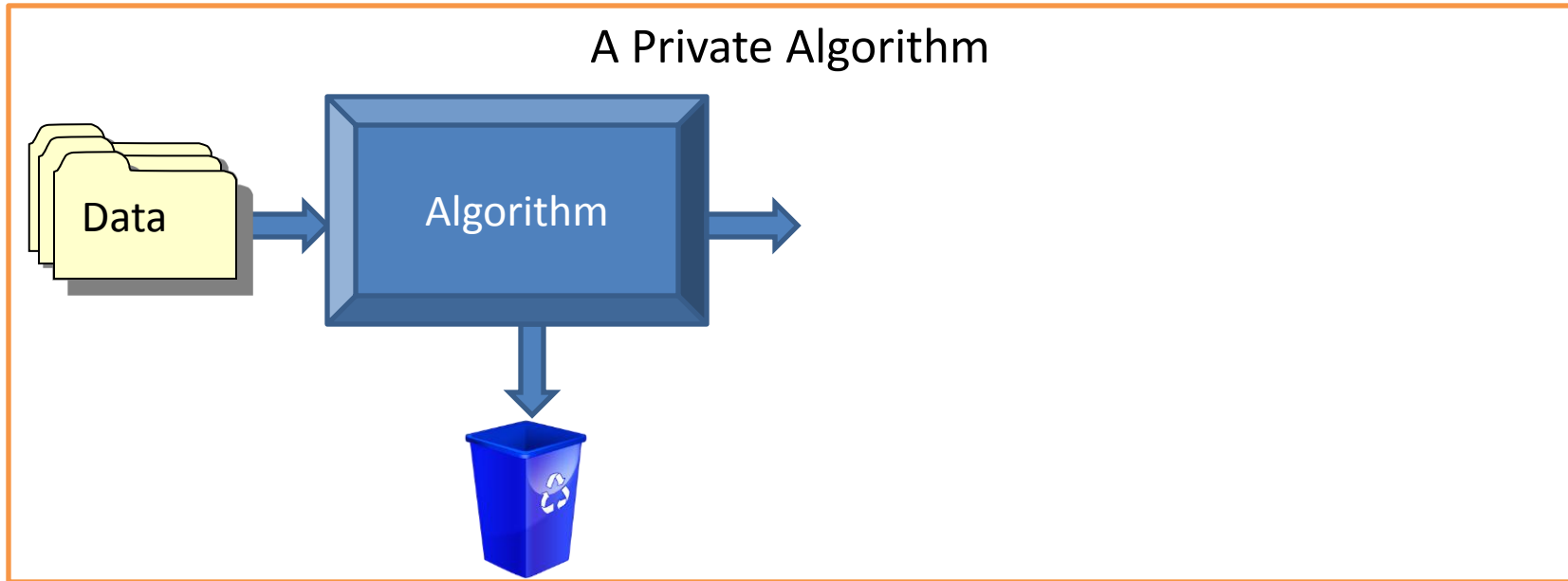
# Why is Differential Privacy “Privacy”?

- $f$  incorporates any auxiliary information an analyst may have about the database now *or in the future*.
- The guarantee is just as strong *even if the analyst knows the entire database except for your value*.
  - A worst case model: no longer any need to reason about what the analyst knows.

# So now we have a definition.

## Course Roadmap

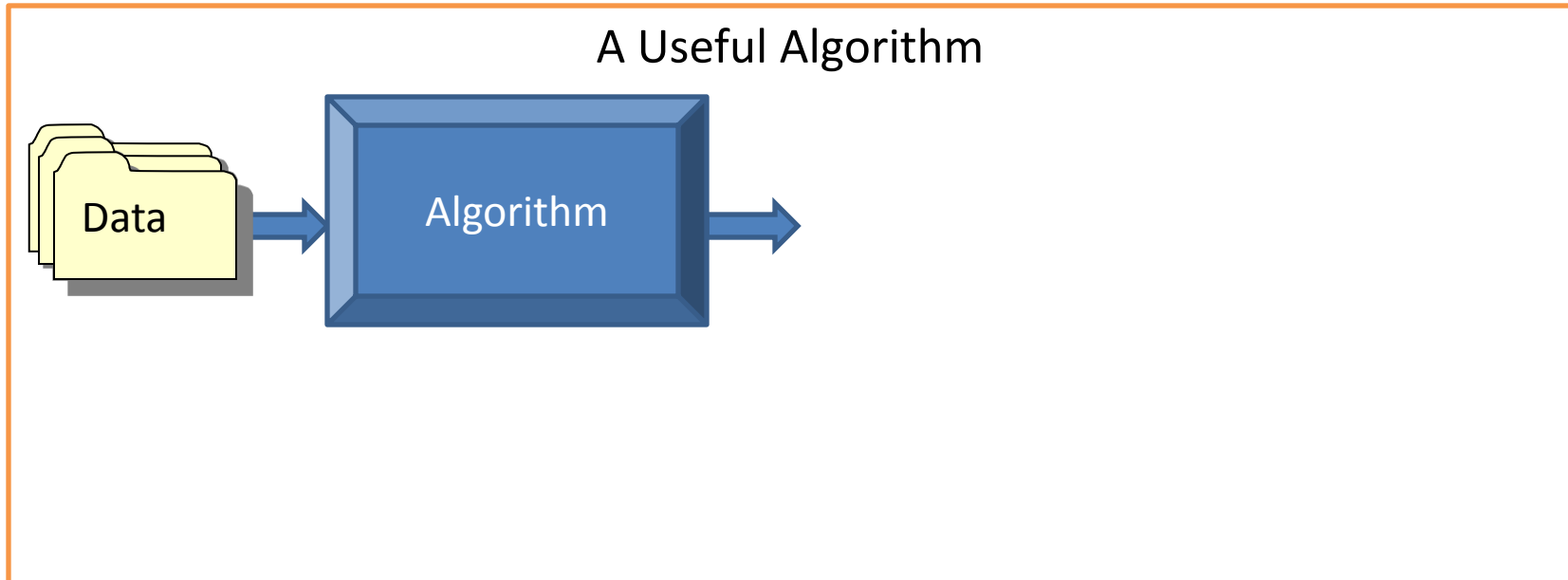
- What are the big questions?
  - How do we trade off privacy and utility?



# So now we have a definition.

## Course Roadmap

- What are the big questions?
  - How do we trade off privacy and utility?



# So now we have a definition.

## Course Roadmap

- How can we build useful, differentially private algorithms?
  - Out of basic building blocks, glued together by composition theorems.

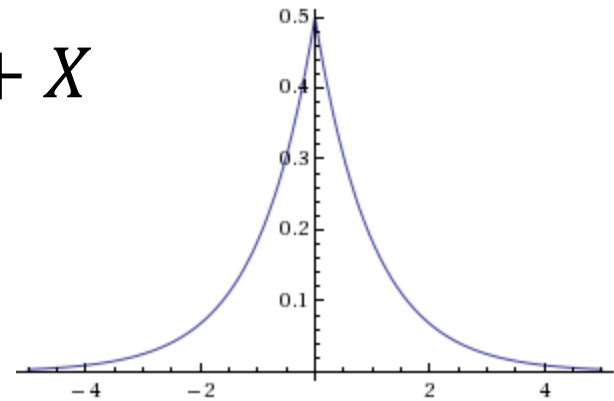
# So now we have a definition.

## Course Roadmap

- Basic Building Blocks
  - Answering numeric queries through perturbation

$$M_f(D) = f(D) + X$$

$$X \sim \text{Lap}\left(\frac{1}{\epsilon}\right)$$



# So now we have a definition.

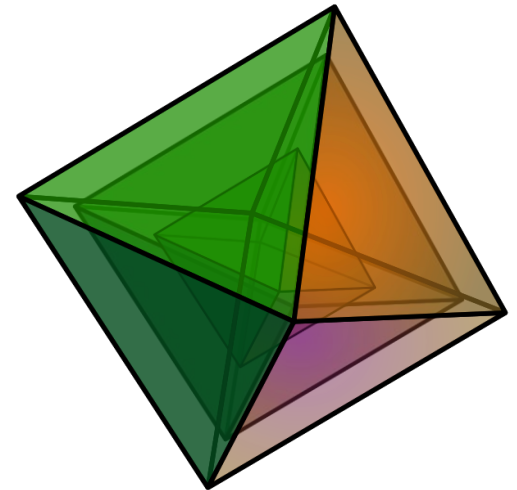
## Course Roadmap

- Basic Building Blocks

- Answering non-numeric queries by sampling from a private distribution

$$M_q(D): 2^X \rightarrow R$$

Output  $r \in R$  with probability  $\sim \exp(-\epsilon q(r, D))$



# So now we have a definition.

## Course Roadmap

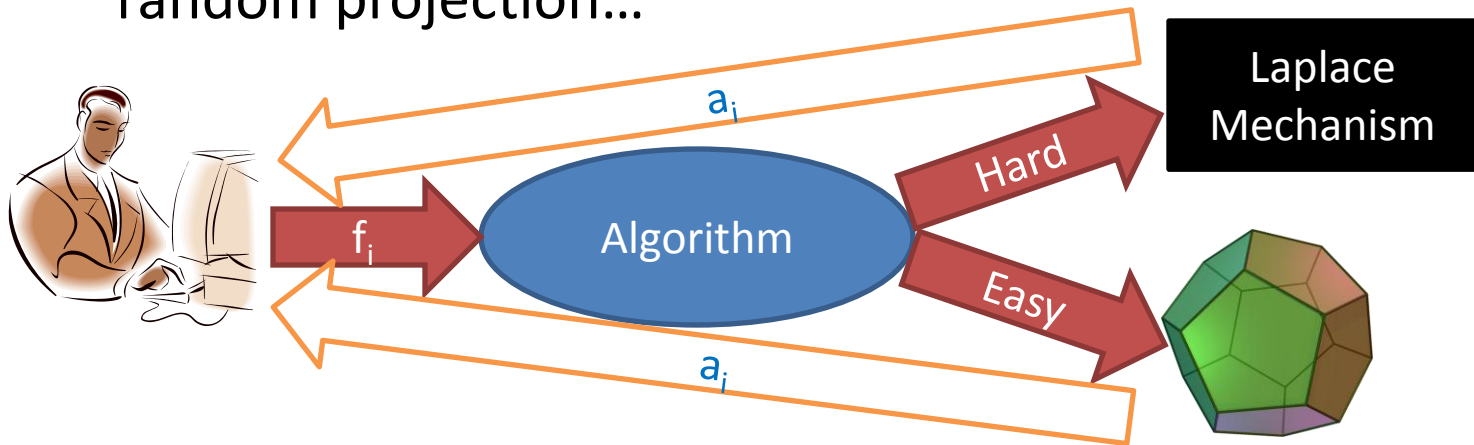
- Combining building blocks into algorithms
  - What are the privacy guarantees for an algorithm  $M$  composed of  $k$  subroutines  $A_1, \dots, A_k$  that are each  $(\epsilon, \delta)$ -differentially private?
    - $(k\epsilon, k\delta)$ -differentially private
    - Also  $\approx (\sqrt{k \log \frac{1}{\delta'}} \epsilon, k\delta + \delta')$ -differentially private
      - Can *trade* lots of  $\epsilon$  for a little more  $\delta$ .



# So now we have a definition.

## Course Roadmap

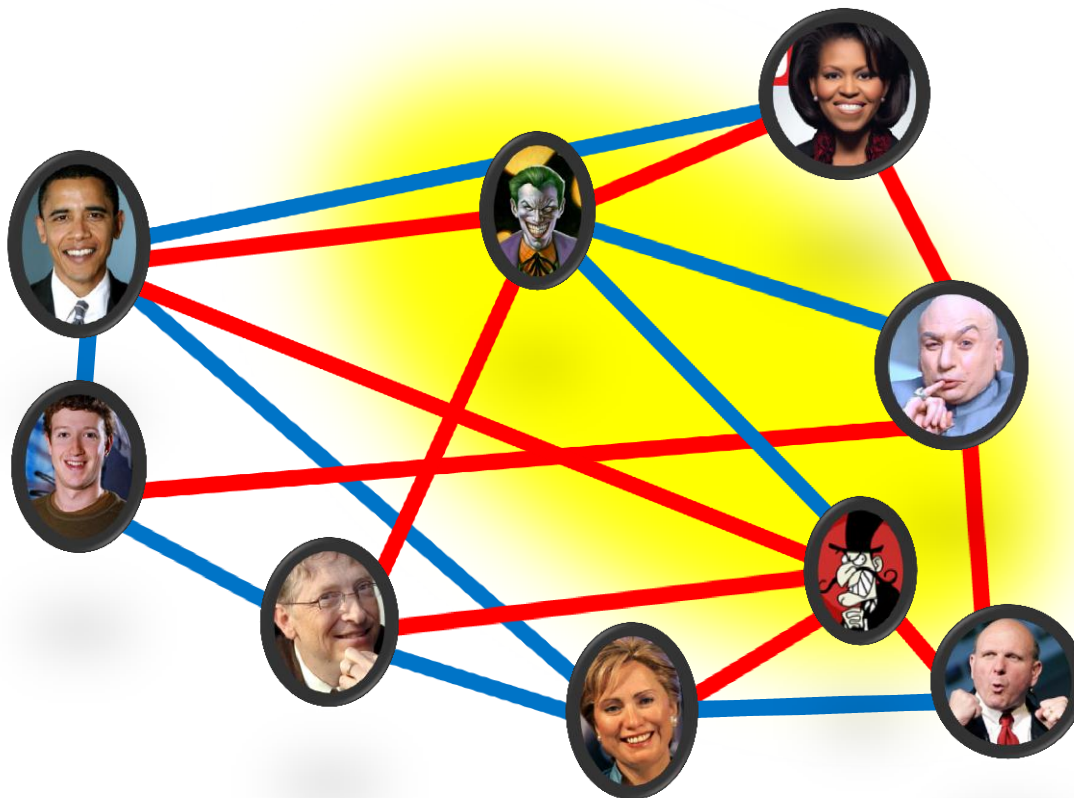
- What can we build?
  - Algorithms for accurately answering *exponentially* many numeric queries in the database size!
    - Leveraging machine learning theory, compression, random projection...



# So now we have a definition.

## Course Roadmap

- What can we build?
  - Algorithms for combinatorial optimization



# So now we have a definition.

## Course Roadmap

- What can we build?
  - Streaming Algorithms
    - That are private even if a hacker is able to look at the internal state of the algorithm.



# So now we have a definition.

## Course Roadmap

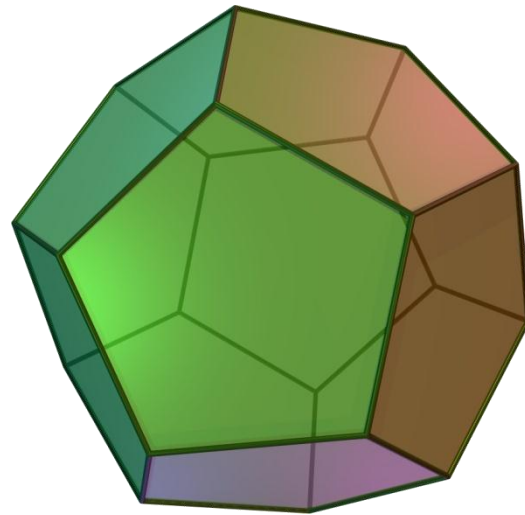
- What can we build?
  - Auctions and truthful mechanisms for privacy-aware economic agents



# So now we have a definition.

## Course Roadmap

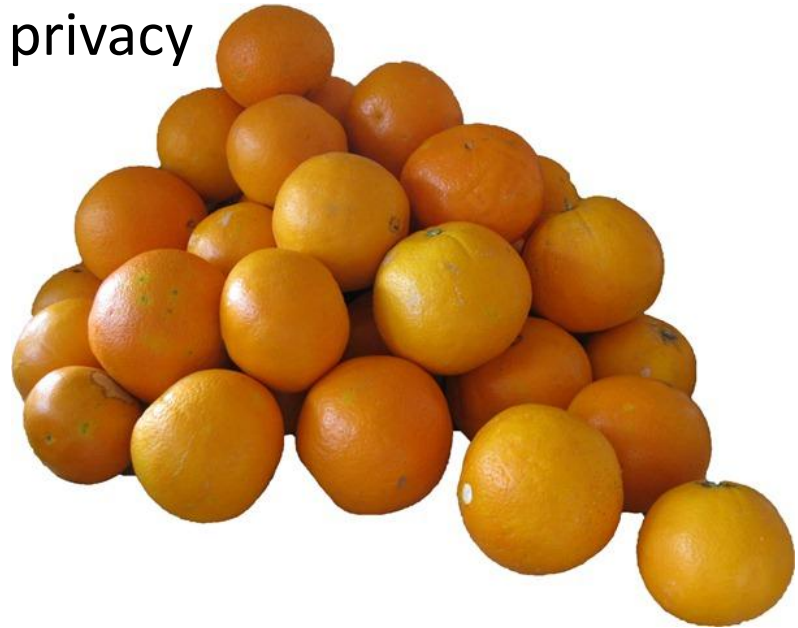
- What *can't* we build?
  - Lower bounds from linear programming
    - Answering queries *too* accurately lets an adversary reconstruct the database



# So now we have a definition.

## Course Roadmap

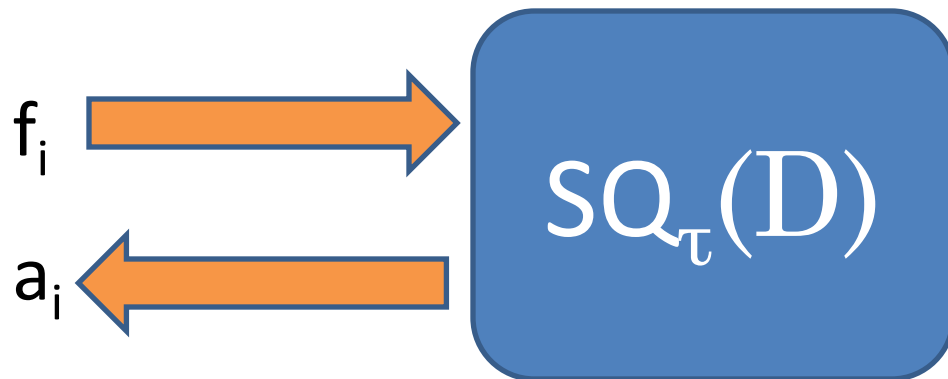
- What *can't* we build?
  - Lower bounds from packing arguments
    - The existence of good *error correcting codes* give lower bounds in differential privacy



# So now we have a definition.

## Course Roadmap

- What *can't* we build?
  - Lower bounds from learning theory
    - Efficient query release algorithms in Kearns' *statistical query* model would lead to too-good-to-be-true learning algorithms.



# To Muse On:

- Think about why differential privacy protects against blatant non-privacy
- Read [Narayanan,Shmatikov06]: How to de-anonymize the Netflix data set.